



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/719,460	12/11/2000	Tomoyuki Asano	450101-02452	8319

20999 7590 11/29/2004

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER

TRAN, TONGOC

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 11/29/2004

9

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/719,460

Applicant(s)

ASANO ET AL.

Examiner

Tongoc Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11 December 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-107 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-107 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>3.6</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This Office Action is in response to Applicant's application serial no. 09/719460.
Claims 1-107 are pending.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 12/11/2000 and 7/23/2002 has been considered by the examiner.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-107 are rejected under 35 U.S.C. 102(e) as being anticipated by Traw et al. (U.S. Patent No. 6,542,610).

In respect to claim 1, Traw discloses an information processing system comprising: a first information processing apparatus comprising an interface having a first transmission mode in which a transmission band is ensured and a second transmission mode in which a transmission band is not ensured, and transmission control means for encrypting data requiring the assurance of the transmission band by a

first encryption key and then transmitting the data in the first transmission mode via the interface and for encrypting related data relating to the data by a second encryption key and then transmitting the related data in the second transmission mode via the interface (e.g. Abstract and col. 10, lines 28-34) ; and

a second information processing apparatus comprising an interface having a first transmission mode in which a transmission band is ensured and a second transmission mode in which a transmission band is not ensured, and receiving control means for decoding, by the first encryption key, the data requiring the assurance of the transmission band which is received in the first transmission mode via the interface and for decoding, by the second encryption key, the related data received in the second transmission mode via the interface (see col. Col. 4, lines 34-58 and col. 10, lines 28-34).

In respect to claim 2, Traw discloses an information processing system as claimed in claim 1, wherein prior to data transmission, a protocol for performing mutual authentication and sharing a plurality of encryption keys between the first information processing apparatus and the second information processing apparatus is executed (e.g. col. 3, lines 20-30 and col. 4, lines 39-58).

In respect to claim 3, Traw discloses the information processing system as claimed in claim 1, wherein music data is transmitted in the first transmission mode and related data relating to the music data is transmitted in the second transmission mode (e.g. .10, lines 27-34).

In respect to claim 4, Traw discloses the information processing system as claimed in claim 1, wherein the first information processing apparatus and the second information processing apparatus are connected with each other via an interface conforming to the IEEE (the Institute of Electrical and Electronics Engineers) 1394 standard, for transmitting data requiring the assurance of a transmission band in an isochronous transmission mode and for transmitting related data relating to the data in an asynchronous transmission mode (e.g. col. 10, lines 27-34).

In respect to claim 5, Traw discloses the information processing system as claimed in claim 4, wherein prior to data transmission, a protocol for performing mutual authentication and sharing a plurality of encryption keys between the first information processing apparatus and the second information processing apparatus is executed in an asynchronous transmission mode (e.g. col. 4, lines 39-58 and col. 6, lines 34-40).

In respect to claim 6, Traw discloses the information processing system as claimed in claim 1, wherein the second information processing apparatus generates two random numbers and transmits them to the first information processing apparatus, the first information processing apparatus generates two random numbers and transmits them to the second information processing apparatus, the first information processing apparatus generates an encryption key used for encrypting the data to be transmitted in the first transmission mode and an encryption key used for encrypting the data to be transmitted in the second transmission mode on the basis of information indicating the validity of the apparatus itself, the generated random number and the received random number, and the second information processing apparatus generates

an encryption key used for decoding the data transmitted in the first transmission mode and an encryption key used for decoding the data transmitted in the second transmission mode on the basis of information indicating the validity of the apparatus itself, the generated random number and the received random number (e.g. col. 6, lines 1-66).

In respect to claim 7, Traw discloses the information processing system as claimed in claim 6, wherein the first information processing apparatus transmits data P generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, to the second information processing apparatus, the second information processing apparatus transmits data Q generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, to the first information processing apparatus, the first information processing apparatus generates an encryption key used for encrypting the data to be transmitted in the first transmission mode and an encryption key used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number is coincident with the received data Q, and the second information processing apparatus generates an encryption key used for decoding the data transmitted in the first transmission mode and an encryption key used for decoding the data transmitted in the second transmission mode in the case where data P' generated on the basis of the information indicating the validity of the

apparatus itself, the generated random number and the received random number is coincident with the received data P (e.g. col. 6, lines 1-67).

In respect to claim 8, Traw discloses the information processing system as claimed in claim 7, wherein the second information processing apparatus generates two random numbers R1 and R2 and transmits them to the first information processing apparatus, the first information processing apparatus generates two random numbers S1 and S2 and transmits them to the second information processing apparatus, the first information processing apparatus transmits data P generated on the basis of information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, to the second information processing apparatus, the second information processing apparatus transmits data Q generated on the basis of information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, to the first information processing apparatus, the first information processing apparatus generates an encryption key K1 used for encrypting the data to be transmitted in the first transmission mode and an encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1 is coincident with the received data Q, and the second information processing apparatus generates an encryption key K'1 used for decoding the data transmitted in the first transmission mode and an encryption key K'2 used for decoding the data transmitted in the second

transmission mode in the case where data P' generated on the basis of the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2 is coincident with the received data P (e.g. col. 6, lines 1-67).

In respect to claim 9, Traw discloses the information processing system as claimed in claim 8, wherein the first information processing apparatus generates the encryption key K1 used for encrypting the data to be transmitted in the first transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1, and generates the encryption key K2 used for encrypting the data to be transmitted in the Second transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, and the second information processing apparatus generates the encryption key K'1 used for decoding the data transmitted in the first transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K'2 used for decoding the data transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2 (e.g. col. 6, lines 1-67 and col. 7, lines 5-55).

In respect to claim 10, Traw discloses the information processing system as claimed in claim 9, wherein the first information processing apparatus transmits data P generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, to the second information processing apparatus, the second information processing apparatus transmits data Q generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, to the second information processing apparatus, the first information processing apparatus generates the encryption key K1 used for encrypting the data to be transmitted in the first transmission mode and the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1 is coincident with the received data Q, and the second information processing apparatus generates the encryption key K' used for decoding the data transmitted in the first transmission mode and the encryption key K'2 used for decoding the data transmitted in the second transmission mode in the case where data P' generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of

the apparatus itself, the received random number S2 and the generated random number R2 is coincident with the received data P (e.g. col. 6, lines 1-67, col. 7, lines 5-55).

In respect to claim 11, Traw discloses the information processing system as claimed in claim 9, wherein the first information processing apparatus and the second information processing apparatus generate the encryption key K1, the encryption key K2, the encryption key K'1 and the encryption key K'2, using a bit value of a part of the result of calculation of the unidirectional function (e.g. col. 6, lines 1-67, col. 7, lines 5-55).

In respect to claim 12, Traw discloses the information processing system as claimed in claim 11, wherein the first information processing apparatus and the second information processing apparatus generate the data P, the data Q', the data Q and the data P', using a bit value of a part of the result of calculation of the unidirectional function (e.g. col. 6, lines 1-67, col. 7, lines 5-55).

In respect to claim 13, discloses the information processing system as claimed in claim 11, wherein the first information processing apparatus and the second information processing apparatus generate the encryption key K1, the encryption key K2, the encryption key K'1 and the encryption key K'2, using a least significant n bits of the result of calculation of the unidirectional function (e.g. col. 6, lines 1-67 and col. 7, lines 5-55).

In respect to claim 14, discloses the information processing system as claimed in claim 13, wherein the first information processing apparatus and the second information processing apparatus generate the data P, the data Q', the data Q and the data P',

using a most significant m bits of the result of calculation of the unidirectional function (e.g. col. 7, lines 5-55).

In respect to claims 15-16, the claim limitations are similar to claims 9-11. Therefore claims 15-16 are rejected based on the similar rationale.

In respect to claim 17, Traw discloses the information processing system as claimed in claim 6, wherein the first information processing apparatus and the second information processing apparatus generate either one of the encryption key used for encrypting the data to be transmitted in the first transmission mode and the encryption key used for encrypting the data to be transmitted in the second transmission mode, on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, and generate the encryption key of the other transmission mode on the basis of the generated encryption key, the generated random number and the received random number (e.g. col. 3, lines 10-30).

In respect to claims 18-27, the claim limitation is similar to claim 7-16. Therefore claim 18 is rejected based on the similar rationale.

In respect to claims 29-54, the claim limitations are method claims that are substantially similar to system claims 1-27. Therefore, claims 29-54 are rejected based on the similar rationale.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

-ITO et al. Disclose a data communication system and method using communication control buses capable of dealing with mixed control and data signals.

-Elgamal et al. Disclose a secure socket layer application program apparatus and method.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00 M-F.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

TT

 November 22, 2004


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100